

**THE DEFINITION OF A
RANDOM SEQUENCE OF
QUBITS: FROM
NONCOMMUTATIVE
ALGORITHMIC PROBABILITY
THEORY TO QUANTUM
ALGORITHMIC INFORMATION
THEORY AND BACK**

Gavriel Segre - University of Pavia, Europe

February 1, 2008

ACKNOWLEDGMENTS:

First of all I want to thank :

- Asterix
- F. Benatti
- C. Calude
- G. Jona-Lasinio
- Obelix
- P. Odifreddi
- M. Rasetti
- A. Rimini
- K. Svozil
- M. Van Lambalgen

for useful discussions and suggestions.

They all have no responsibility for any mistake contained in these pages.

Contents

1	Introduction	3
2	Strings and sequences over commutative and noncommutative alphabets	3
3	The randomness of repeated classical and quantum coin tossings	3
4	Martin-Löf random sequences over a commutative alphabet	3
5	The difference between commutativity / noncommutativity of the computational device and commutativity / noncommutativity of the computed objects	3
6	Quantum Algorithmic Information Theory and the Pour El extension of Church	

Thesis 3

- 7 Looking for Martin-Löf physically-quantum
randomness: an issue of Algorithmic
Free Probability Theory 4**

1 Introduction

Equivalent approaches to the definition of a random sequence over a **(commutative) finite alphabet** Σ :

- *Chaitin's definition* [Cha69a], [Cha69b], [Cha87], [Cal94], [Vit97]:

algorithmic incompressibility in the framework of **(Commutative) Algorithmic Information Theory**

- *definition by Martin-Löf tests* [ML66a], [ML66b], [Cha87], [Cal94], [Vit97]:

passage of all the algorithmically implementable (commutative) statistical tests

- *Martin-Löf's algorithmic measure-theoretic definition [ML66a], [ML66b], [Cha87], [Cal94], [Vit97]:*

not belongness to any set of null algorithmic (commutative) unbiased probability

- *Solovay's algorithmic measure-theoretic definition [Sol77], [Cal94], [Vit97]*
- *some (still lacking!) restriction of Von-Mises-Church's definition [Mis81], [Chu40], [Lon92], [Vit97]:*

stability of the relative-frequencies of the various (commutative) letters under the extraction of a subsequence by a properly subset of the (commutative) algorithmic place selection rules

Common feauture of all these definitions:

*THEY CONTAIN THE TERM
ALGORITHMIC AND , THUS, DEPEND ON
COMPUTABILITY THEORY*

*This suggest that the same should happen also for
the definition of a random sequence on a
noncommutative finite alphabet Σ_{NC}*

Conceptual meaning of the inelusibility of
Computability Theory:

COMMUTATIVE MEASURE THEORY

*can't resolve by itself the definition of a random
sequence on a commutative alphabet suggesting the
requirement of an alternative **ALGORITHMIC
FOUNDATION OF COMMUTATIVE
PROBABILITY THEORY** deeply pursued by
the same father of the measure-theoretic
foundation A.N. Kolmogorov [Shi93]*

*This suggest that the same should be true as to
NONCOMMUTATIVE PROBABILITY
leading to the idea of pursuing an
**ALGORITHMIC FOUNDATION OF
NONCOMMUTATIVE PROBABILITY
THEORY***

The individuation of the **correct noncommutative generalization of Martin-Löf definition** should be equivalent to the characterization of a random sequence on a noncommutative alphabet as **algorithmic incompressible** in the framework of **Quantum Algorithmic Information Theory** [Svo96], [Man],[Vit99], [vDSL00] giving some light on the nature of such a theory.

2 Strings and sequences over commutative and noncommutative alphabets

Given the commutative alphabet of one cbit
 $\Sigma \equiv \{0, 1\}$:

DEFINITION 2.1

SET OF THE STRINGS ON Σ :

$$\Sigma^* \equiv \cup_{k \in \mathbb{N}} \Sigma^k \quad (2.1)$$

DEFINITION 2.2

SET OF THE SEQUENCES ON Σ :

$$\Sigma^\infty \equiv \{\bar{x} : \mathbb{N}_+ \rightarrow \Sigma\} \quad (2.2)$$

Theorem 2.1

(ON THE CARDINALITIES OF STRINGS AND SEQUENCES)

$$\textit{cardinality}(\Sigma^*) = \aleph_0 \quad (2.3)$$

$$\textit{cardinality}(\Sigma^\infty) = \aleph_1 \quad (2.4)$$

Remark 2.1

ON THE ASSUMPTION OF NOT
INTERMEDIATE DEGREES OF INFINITY
BETWEEN Σ^* AND Σ^∞

I will assume from now on the following:

AXIOM 2.1

CONTINUUM HYPOTHESIS:

$$2^{\aleph_0} = \aleph_1 \quad (2.5)$$

that is well known to be **consistent** but
independent from the formal system of Zermelo
- Fraenkel endowed with the Axiom of Choice
(ZFC) giving foundation to Mathematics [Odi89]

DEFINITION 2.3

DIADIC EXPANSION:

$$\begin{aligned} de : \Sigma^\infty &\rightarrow [0, 1] \\ de(x_1, x_2, \dots) &= \sum_{n=1}^{\infty} \frac{x_n}{2^n} \end{aligned} \quad (2.6)$$

Remark 2.2

NOT BIJECTIVITY OF THE DIADIC EXPANSION:

de is injective but not surjective since each point of the closed unitary interval has two counter images: one *terminating* and one *nonterminating*; e.g.:

$$de^{-1}\left(\frac{1}{2}\right) = \{100000\dots, 011111\dots\} \quad (2.7)$$

DEFINITION 2.4

CYLINDER SET W.R.T. $\vec{x} = (x_1, \dots, x_n) \in \Sigma^*$:

$$\Gamma_{\vec{x}} \equiv \{\bar{y} = (y_1, y_2, \dots) \in \Sigma^\infty : \\ y_1 = x_1, \dots, y_n = x_n\} \quad (2.8)$$

DEFINITION 2.5

CYLINDER - σ - ALGEBRA ON Σ^∞ :

$$\mathcal{F}_{cylinder} \equiv \sigma\text{-algebra generated by } \{\Gamma_{\vec{x}} : \vec{x} \in \Sigma^*\} \\ (2.9)$$

DEFINITION 2.6

LEBESGUE UNBIASED PROBABILITY
MEASURE ON Σ^∞ :

$$P_{unbiased}(A) \equiv \mu_{Lebesgue}(de(A)) \quad A \in \mathcal{F}_{Borel} \\ (2.10)$$

Remark 2.3

THE UNBIASED PROBABILITY SPACE OF ALL THE SEQUENCES OF CBITS AS DIRECT PRODUCT OF UNBIASED PROBABILITY SPACES EACH FOR EVERY SINGLE CBIT:

The unbiased probability space $(\Sigma^\infty, P_{unbiased})$ of all the sequences of cbits may be expressed as:

$$\begin{aligned} (\Sigma^\infty, P_{unbiased}) &= \times_{n \in \mathbb{Z}} (\Sigma, C_{\frac{1}{2}, \frac{1}{2}}) \\ C_{\frac{1}{2}, \frac{1}{2}}(x) &\equiv \frac{1}{2} \quad x \in \Sigma \end{aligned} \tag{2.11}$$

Remark 2.4

THE UNBIASED PROBABILITY SPACE OF ALL THE SEQUENCES OF CBITS AS A DEGENERATE NONCOMMUTATIVE PROBABILITY SPACE:

By the **Gelfand isomorphism** the classical probability space $(\Sigma^\infty, P_{unbiased})$ may be equivalently seen as the degenerate **noncommutative probability space** (or **quantum probability space** or **W^* -algebraic probability space**, or \dots [Par92], [Opr94], [Mey95], [Pet93], [Ohy97], [Pet00]) $(L^\infty(\Sigma^\infty, P_{unbiased}), \tau_{unbiased})$ where $\tau_{unbiased}$ is the tracial state on the Von Neumann algebra [Sun87] $L^\infty(\Sigma^\infty, P_{unbiased})$ defined as:

$$\tau_{unbiased}(f) \equiv \int_{\Sigma^\infty} f(x) dP_{unbiased} \quad (2.12)$$

Remark 2.5

THE KEY METAPHORE OF NONCOMMUTATIVE PROBABILITY THEORY AND THE NONCOMMUTATIVE ALPHABET OF ONE QUBIT

The key metaphore of Noncommutative Probability Theory consists in imaging an illusionary noncommutative corrispective of the Gelfand-Theorem and looking to a noncommutative probability space (A, ω) as a sort of $(L^\infty(SPAC E_{NC}, P_{NC}), \int_{SPAC E_{NC}} dP_{NC})$.

So the **one-qubit** W^* – algebra $M_2(\mathbb{C})$ endowed with some state may be identified as the set of the properly-smooth functions over the

**NONCOMMUTATIVE ALPHABET OF
ONE CBIT** : $\Sigma_{NC} \equiv \{0, 1\}_{NC}$

DEFINITION 2.7

UNBIASED NONCOMMUTATIVE
PROBABILITY SPACE ON THE ONE QUBIT
ALPHABET Σ_{NC} :

$$(M_2(\mathbb{C}), \tau_2)$$
$$\tau_2\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right) \equiv \frac{1}{2}(a_{11} + a_{22}) \quad (2.13)$$

DEFINITION 2.8

SET OF THE SEQUENCES ON Σ_{NC} :

$$L^\infty(\Sigma_{NC}^\infty) \equiv s - closure(\otimes_{n \in \mathbb{N}} M_2(\mathbb{C})) \quad (2.14)$$

$L^\infty(\Sigma_{NC}^\infty)$ is a **II_1 -factor** and thus has a canonical (i.e. finite, normal and faithful) trace, namely:

$$\tau_{unbiased} \equiv \bigotimes_{n \in \mathbb{N}} \tau_2 \quad (2.15)$$

DEFINITION 2.9

UNBIASED NONCOMMUTATIVE
PROBABILITY SPACE OF ALL THE
SEQUENCES OF QUBITS:

$$(L^\infty(\Sigma_{NC}^\infty) , \tau_{unbiased})$$

3 The randomness of repeated classical and quantum coin tossings

The correct Martin Löf - Solovay - Chaitin definition of a random sequence on Σ [ML66a], [ML66b], [Sol77], [Cha87], [Cal94], [Vit97] satisfies the following intuitive condition:

CONSTRAINT 3.1

ON THE NOTION OF A RANDOM SEQUENCE
ON THE COMMUTATIVE ALPHABET Σ :

*Making infinite **independent** trials of the experiment consisting on tossing a **classical coin** we must obtain a random sequence with probability one*

So a reasonable strategy to identify the correct definition of a random sequence of qubits would consist in:

- formulating an analogous constraint in terms of an infinite sequence of experiments consisting in tossing a quantum coin
- identifying the information that such a constraint gives on the correct way of making a noncommutative generalization of Martin-Löf's algorithmic-measure-theoretic definition

The commutative random variables $\mathbf{c}_{\mathbf{t}_1}$ and $\mathbf{c}_{\mathbf{t}_2}$ on the commutative probability space $(L^\infty(\Sigma^\infty, P_{unbiased}), \tau_{unbiased})$ representing the results of the classical-coin tossing at times, respectively, \mathbf{t}_1 and \mathbf{t}_2 are assumed to be **independent**:

$$\begin{aligned} \tau_{unbiased}(c_{t_1}^n c_{t_2}^m) &= \\ \tau_{unbiased}(c_{t_1}^n) \tau_{unbiased}(c_{t_2}^m) \quad \forall n, m \in \mathbb{N} \end{aligned} \quad (3.1)$$

Such a condition, anyway, requires that c_{t_1} and c_{t_2} are commuting among themselves :

$$[c_{t_1}, c_{t_2}] = 0 \quad (3.2)$$

But such a condition can't, clearly, be true for the noncommutative random variables $\tilde{\mathbf{c}}_{\mathbf{t}_1}$ and $\tilde{\mathbf{c}}_{\mathbf{t}_2}$ on the noncommutative probability space $(L^\infty(\Sigma_{NC}^\infty), \tau_{unbiased})$ representing the results of quantum-coin tossing at times, respectively, \mathbf{t}_1 and \mathbf{t}_2 having any **noncommutative correlation** among themselves.

The natural corrispective of the notion of **independence** for two generic noncommutative random variables \mathbf{x} and \mathbf{y} over a noncommutative probability space (A, ω) is Dan Virgil Voiculescu's notion of **freeness** [Pet00] stating that there doesn't exist any particular **relation** linking \mathbf{x} and \mathbf{y} besides the fact of belonging to the same W^* -algebra exactly as happens for two generators of a **free group**.

Remark 3.1

FREENESS IMPLIES NOT INDEPENDENCE

Since among the excluded particular relations among \mathbf{x} and \mathbf{y} there is also the one stating the compatibility of such random variables, if \mathbf{x} and \mathbf{y} are **free** they can't be **independent**

DEFINITION 3.1

THE NONCOMMUTATIVE RANDOM
VARIABLES \mathbf{x} AND \mathbf{y} ON THE
NONCOMMUTATIVE PROBABILITY SPACE
 (A, ω) ARE FREE:

$$\forall n \in \mathbb{N}, \forall i_1, \dots, i_n \in \{1, 2\} :$$

$$i(k) \neq i(k+1) (1 \leq k \leq n-1)$$

$$\omega(a_1 \cdots a_n) = 0 \text{ whenever } a_k \in A_{i(k)},$$

$$\omega(a_k) = 0, 1 \leq k \leq n$$

$$A_1 \equiv \text{generated}(x)$$

$$A_2 \equiv \text{generated}(y) \quad (3.3)$$

Returning now to the noncommutative random variables $\tilde{\mathbf{c}}_{\mathbf{t}_1}$ and $\tilde{\mathbf{c}}_{\mathbf{t}_2}$ on the noncommutative probability space $(L^\infty(\Sigma_{NC}^\infty), \tau_{unbiased})$ representing the results of the quantum-coin tossing at times, respectively, \mathbf{t}_1 and \mathbf{t}_2 it appears natural to assume that they are **free**.

Remark 3.2

The notion of **freeness** is an equivalence relation on the noncommutative probability space (A, ω) and thus extends immediately to an arbitrary number of noncommutative random variables.

It appears then natural to require that the notion of **noncommutative algorithmic randomness** we are looking for obeys the following:

CONSTRAINT 3.2

ON THE NOTION OF A RANDOM SEQUENCE
ON THE NONCOMMUTATIVE ALPHABET Σ_{NC} :

*Making infinite **free** trials of the experiment consisting on tossing a **quantum coin** we must obtain a random sequence with noncommutative probability one*

4 Martin-Löf random sequences over a commutative alphabet

DEFINITION 4.1

n^{th} PREFIX OF THE SEQUENCE $\bar{x} \in \Sigma^\infty$:

$$\vec{x}(n) \in \Sigma^n : \exists \bar{y} \in \Sigma^\infty : \bar{x} = \vec{x}(n) \cdot \bar{y} \quad (4.1)$$

DEFINITION 4.2

SEQUENCES BEGINNING WITH $S \subset \Sigma^*$:

$$S\Sigma^\infty \equiv \{ \bar{x} \in \Sigma^\infty : \vec{x}(n) \in S, n \in \mathbb{N}_+ \} \quad (4.2)$$

Endowed Σ^∞ with the **product topology**
induced by the **discrete topology** of Σ :

DEFINITION 4.3

$S \subset \Sigma^\infty$ IS A NULL SET:

$\forall \epsilon > 0, \exists G_\epsilon \subset \Sigma^\infty$ *open* :

$$(S \subset G_\epsilon) \text{ and } (P_{unbiased}(G_\epsilon) < \epsilon) \quad (4.3)$$

DEFINITION 4.4

UNARY PREDICATES ON Σ^∞ :

$$\mathcal{P}(\Sigma^\infty) \equiv \{p_{\bar{x}} : \text{predicate about } \bar{x} \in \Sigma^\infty\} \quad (4.4)$$

DEFINITION 4.5

TYPICAL PROPERTIES OF Σ^∞ :

$$\begin{aligned} \mathcal{P}(\Sigma^\infty)_{TYPICAL} &\equiv \{p_{\bar{x}} \in \mathcal{P}(\Sigma^\infty) : \\ &\{\bar{x} \in \Sigma^\infty : p_{\bar{x}} \text{ doesn't hold} \} \text{ is a null set} \} \end{aligned} \quad (4.5)$$

Denoted by $RANDOM(\Sigma^\infty)$ the set of random sequences over Σ we can restate the constraint 3.1 as:

CONSTRAINT 4.1

ON THE DEFINITION OF $RANDOM(\Sigma^\infty)$:

the unary predicate

$p_{\bar{x}} \equiv \langle\langle \bar{x} \in RANDOM(\Sigma^\infty) \rangle\rangle$ *is a typical property of Σ^∞ , i.e. $p_{\bar{x}} \in \mathcal{P}(\Sigma^\infty)_{TYPICAL}$*

Remark 4.1

Such a constraint doesn't identify $RANDOM(\Sigma^\infty)$.

It would appear natural to try to characterize the random sequences over Σ in a purely measure-theoretic way by the following:

DEFINITION 4.6

$$\begin{aligned} RANDOM(\Sigma^\infty)_{\text{purely-measure-theoretic}} &\equiv \\ \{\bar{x} \in \Sigma^\infty : p_{\bar{x}} \text{ holds } \forall p \in \mathcal{P}(\Sigma^\infty)_{\text{TYPICAL}}\} &\quad (4.6) \end{aligned}$$

But such a way can't be pursued owing to the following:

Theorem 4.1

ON THE IMPOSSIBILITY OF ABSOLUTE CONFORMISM:

$$\begin{aligned} RANDOM(\Sigma^\infty)_{\text{purely-measure-theoretic}} &= \emptyset \\ &\quad (4.7) \end{aligned}$$

PROOF:

Following Calude's diagonalization proof [Cal94] let us consider the following family of unary predicates over Σ^∞ depending on the parameter $\bar{y} \in \Sigma^\infty$:

$$p_{\bar{y}}(\bar{x}) \equiv \begin{aligned} &<< \forall n \in \mathbb{N}_+ \exists m \in \mathbb{N}_+ : \\ &m \geq n \text{ and } \bar{x}_m \neq \bar{y}_m >> \end{aligned} \quad (4.8)$$

Clearly:

$$P_{unbiased}(\{\bar{x} \in \Sigma^\infty : p_{\bar{x}, \bar{y}} \text{ doesn't hold}\}) = 0 \quad \forall \bar{y} \in \Sigma^\infty \quad (4.9)$$

and so:

$$p_{\bar{y}} \in \mathcal{P}(\Sigma^\infty)_{TYPICAL} \quad \forall \bar{y} \in \Sigma^\infty \quad (4.10)$$

Anyway:

$$p_{\bar{x}}(\bar{x}) \text{ doesn't hold} \quad \forall \bar{x} \in \Sigma^\infty \quad (4.11)$$

implying the formula eq.4.7 ■

Remark 4.2

CONCEPTUAL DEEPNESS OF MARTIN-LÖF'S RESULT

The theorem 4.1 shows that we have to relax the condition that a random sequence possesses **all the typical properties** requiring only that it satisfies a **proper subclass of typical properties**.

One could, at this point, think that a meaningful restriction could be obtained again in a purely measure-theoretic framework, e.g. posing constraints on some kind of speed of convergence to zero of the unbiased probability of the accepted typical properties.

*ANYWAY MARTIN-LÖF SHOWED THAT THE
RIGHT CRITERIUM OF SELECTION OF THE
PROPER SUBCLASS DEFINITELY DOESN'T
BELONG TO MEASURE THEORY BUT TO
COMPUTABILITY THEORY :*

**THE CONSIDERED TYPICAL
PROPERTIES MUST BE TESTABLE IN
AN *EFFECTIVELY-COMPUTABLE*
WAY**

Remark 4.3

MARTIN-LÖF CONDITION LIES WITHIN THE BOUNDARIES OF CLASSICAL RECURSION THEORY

By the theorem 2.1:

- Computability Theory on Σ^* lies within the boundaries of **Classical Recursion Theory** [Odi89]
- Computability Theory on Σ^∞ lies outside the boundaries of **Classical Recursion Theory**

Although the definition of a random sequence regards Σ^∞ Martin-Löf's constraint of effective-computability of the relevant typical properties is implementable thoroughly in terms of Computability Theory on Σ^* and then belongs to **Classical Recursion Theory** whose firm foundation lies on the theoretic and experimental evidence lying behind the assumption of **Church's Thesis** [Odi89], [Odi96].

DEFINITION 4.7

$S \subset \Sigma^\infty$ IS ALGORITHMICALLY-OPEN:

$(S \text{ is open }) \text{ and } (S = X\Sigma^\infty$

$X \text{ recursively – enumerable}) \quad (4.12)$

DEFINITION 4.8

ALGORITHMIC SEQUENCE OF
ALGORITHMICALLY-OPEN SETS:

a sequence $\{S_n\}_{n \geq 1}$ of algorithmically open sets

$S_n = X_n \Sigma^\infty : \exists X \subset \Sigma^* \times \mathbb{N}$ **recursively enumerable** with:

$$X_n = \{\vec{x} \in \Sigma^* : (\vec{x}, n) \in X\} \quad \forall n \in \mathbb{N}_+$$

DEFINITION 4.9

$S \subset \Sigma^\infty$ IS AN ALGORITHMICALLY-NULL SET:

$\exists \{G_n\}_{n \geq 1}$ algorithmic sequence of algorithmically-open sets :

$$S \subset \bigcap_{n \geq 1} G_n$$

and:

$$\text{alg} - \lim_{n \rightarrow \infty} P_{unbiased}(G_n) = 0$$

i.e. there exist and increasing, unbounded,

recursive function $f : \mathbb{N} \rightarrow \mathbb{N}$ so that

$$P_{unbiased}(G_n) < \frac{1}{2^k} \text{ whenever } n \geq f(k)$$

DEFINITION 4.10

RANDOM SEQUENCES OVER THE
COMMUTATIVE ALPHABET Σ :

$$\begin{aligned} \textit{RANDOM}(\Sigma^\infty) &\equiv \\ \Sigma^\infty - \{S \subset \Sigma^\infty \text{ algorithmically null } \} &\quad (4.13) \end{aligned}$$

5 The difference between commutativity / noncommutativity of the computational device and commutativity / noncommutativity of the computed objects

Remark 5.1

CONFUSION BETWEEN SUBJECT AND
OBJECT OF COMPUTATION:

There exists in the literature a partial confusion between the **attributes of the computational device** and the **attributes of the computed mathematical objects**.

Hence some property (classicality/quantisticality
i.e. commutativity/noncommutativity) is used in
two undistinguished (and often interchanged)
acceptions according to it refers:

- to the **subject of the computation**, i.e. to
the computational device
- to the **object of the computation**, i.e. to
the computed mathematical objects

Remark 5.2

Any issue of Computability Theory must analyze separately each cell of the following:

DIAGRAM 5.1

DIAGRAM OF COMPUTATION:

$\frac{OBJECT}{SUBJECT}$	C_M	NC_M
C_Φ	\cdot_{11}	\cdot_{12}
NC_Φ	\cdot_{21}	\cdot_{22}

with:

C_M : MATHEMATICALLY CLASSICAL

NC_M : MATHEMATICALLY NONCLASSICAL

C_Φ : PHYSICALLY CLASSICAL

NC_Φ : PHYSICALLY NONCLASSICAL

1^{th} ISSUE: WHO IS COMPUTABLE ?

- $cell_{11} : C_M \cap C_\Phi$

There is complete agreement in the scientific community that, as to the computation by **physically classical computers** of the following set of functions:

DEFINITION 5.1

MATHEMATICALLY CLASSICAL
FUNCTIONS:

(partial) functions on sets $S : card(S) \leq \aleph_0$

Church's Thesis holds leading to the identification of the computable (partial) functions with the (partial) recursive functions [Odi89], [Odi96]

- $cell_{21} : C_M \cap NC_\Phi$

There is no universally accepted answer in the scientific community to the question if a **physically nonclassical computer** can violate Church's Thesis, i.e. can compute non-recursive **mathematically classical functions**.

In particular, as far as the computation by **physically quantistical computers of mathematically classical functions** is concerned, the common opinion among the leading researchers in Quantum Computation [Fey82], [Deu85], [Joz98] is that **Nonrelativistic Quantum Mechanics and Partially-relativistic Quantum Mechanics (Local Quantum Field Theories)** don't violate Church's Thesis.

Finally, when **Generally-relativistic Quantum Mechanics** (both in the form of **quantum Gravity** and in the form of some suggested **gravitationally-modificated Quantum Mechanics**) is considered, the whole story touches the strongly debated ideas of R. Penrose [Pen89], [Pen96]

- $cell_{12} : NC_M \cap C_\Phi$

As soon as one goes out from the boundaries of Classical Recursion Theory the almost miraculous equivalence of all the different approaches, that in such a theory manifests the strong experimental verification of Church's Thesis, dramatically disappears.

Just as to the Computability Theory by **physically classical computers** of (partial) functions on sets $S : card(S) = \aleph_1$ many different inequivalent candidate theories have been proposed:

1. the Standard Theory generated by the studies of Grzegorczyck - Lacombe [Ric89]
2. the theory developed by the so called Markov School in the framework of Constructive Mathematics [Odi89]
3. the Blum - Shub - Smale 's Theory [Sma92], [S.S98]

The relative popularity of the issue about the concurrence of such candidate theories is owed to Penrose's question if Mandelbrot set is recursive [Pen89].

Given a **noncommutative probability space**
 (A, ω) :

DEFINITION 5.2

AUTOMORPHISMS OF A :

$$Aut(A) \equiv \{ \alpha : \text{involutive morphisms of } A \} \quad (5.1)$$

DEFINITION 5.3

DYNAMICS OF (A, ω) [Ben93]:

$$DYN[(A, \omega)] \equiv \{ \alpha \in Aut(A) : \\ \omega(\alpha(a)) = \omega(a) \ \forall a \in A \} \quad (5.2)$$

DEFINITION 5.4

C_ϕ - COMPUTABLE AUTOMORPHISMS OF
A:

$$\begin{aligned} C_\phi - AUT(A) &\equiv \\ &\{\alpha \in AUT(A) : \\ &\alpha \text{ is computable by } \textit{classical}_\Phi \text{ computers}\} \quad (5.3) \end{aligned}$$

DEFINITION 5.5

C_ϕ - COMPUTABLE-DYNAMICS OF (A, ω) :

$$\begin{aligned} C_\phi - DYN[(A, \omega)] &\equiv \\ &\{\alpha \in DYN[(A, \omega)] : \\ &\alpha \text{ is computable by } \textit{classical}_\Phi \text{ computers}\} \quad (5.4) \end{aligned}$$

- $cell_{22} : NC_M \cap NC_\Phi$

It's important to realize that Church Thesis doesn't imply that the answer to the 1^{th} *ISSUE* contained in the cells $cell_{12}$ and $cell_{22}$ must be equal.

For example Church Thesis is not incompatible with an hypothetical situation in which Mandelbrot set would be C_Φ - incomputable but NC_Φ - computable

In the same way , given a **noncommutative probability space** (A, ω) and introduced the following notions:

DEFINITION 5.6

NC_ϕ - COMPUTABLE AUTOMORPHISMS OF A:

$$NC_\phi - AUT(A) \equiv$$

$$\{\alpha \in AUT(A) :$$

$$\alpha \text{ is computable by } nonclassical_\Phi \text{ computers}\}$$

(5.5)

DEFINITION 5.7

NC_ϕ - COMPUTABLE-DYNAMICS OF (A, ω) :

$$NC_\phi - DYN[(A, \omega)] \equiv \{\alpha \in DYN[(A, \omega)] :$$

$$\alpha \text{ is computable by } nonclassical_\Phi \text{ computers}\}$$

(5.6)

we have that:

Church Thesis \Rightarrow

$$(C_\phi - AUT(A) = NC_\phi AUT(A)) \quad (5.7)$$

Church Thesis \Rightarrow

$$(C_\phi - DYN[(A, \omega)] = NC_\phi - DYN[(A, \omega)]) \quad (5.8)$$

2^{th} ISSUE: WHO IS EFFICIENTLY COMPUTABLE ?

The deep scientific revolution brought by Quantum Computation is that:

Computational Complexity Theory is not a purely mathematical theory [Odi99] in that the answers it gives are different on the 1^{th} and the 2^{th} rows of the diagram 5.1

as is ultimately implied by the complexity class relations [Vaz97], [Cle98]:

$$P \subset QP \quad (5.9)$$

$$ZPP \subset ZQP \quad (5.10)$$

Remark 5.3

QUANTUM DICE DIFFERS BOTH FROM CLASSICAL DICE AND FROM CLASSICAL ANAΓKH

The relations eq.5.9, eq.5.10 show that deep peculiarity of the statistical structure of Quantum Mechanics [Hol99]:

they ultimately imply that, under the assumption $P \neq NP$ [Odi99], **quantum nondeterminism** is different both from **classical determinism** and from **classical nondeterminism**.

Unfortunately such an issue has not been considered yet in all the discussions about the possibility of a deterministic completion of Quantum Mechanics [Zur83], [Bel93], [Per95], [Hil93], [Svo98], [Aul00]

FUNDAMENTAL QUESTION :

**DOES ALGORITHMIC INFORMATION
THEORY DIFFERS IN THE 1^{TH} AND IN
THE 2^{TH} ROWS OF THE DIAGRAM5.1 ?**

Remark 5.4

ARGUMENT TO ANSWER $\langle\langle YES \rangle\rangle$ TO
THE **FUNDAMENTAL QUESTION**:

By the link existing between **Computational Complexity Theory** and **Algorithmic Information Theory** (passing, mainly, through **resource-bounded algorithmic information** [Lon92], [Cal94], [Vit97]) and the relations eq.5.9, eq.5.10

6 Quantum Algorithmic Information Theory and the Pour El extension of Church Thesis

Remark 6.1

ARGUMENT TO ANSWER $\langle\langle NO \rangle\rangle$ TO THE **FUNDAMENTAL QUESTION**:

If one assumed that:

1. **Quantum Algorithmic Information Theory** must satisfy **Uspensky's Axiomatic Construction** [Usp92]
2. **Pour El Thesis** [PE99] holds

it would follow that for finite dimensional quantum systems the answer to the fundamental question is $\langle\langle no \rangle\rangle$.

Algorithmic Information Theory , i.e. the theory dealing with the algorithmic information of an object defined as the length of the shortest algorithm calculating it, has been originally defined for sets of objects with cardinality at most \aleph_0 [Cal94].

A generalization of such a theory have been proposed by Vladimir A. Uspensky through the introduction of an axiomatic procedure by which Algorithmic Information Theory may be constructed on any set of objects satisfying certain properties.

Demanding to the original Uspensky's article [Usp92] for details I will briefly review here what I will call from now on Uspensky's Axiomatic Procedure.

Given a set S let us introduce the following definitions:

DEFINITION 6.1

LENGTH ON S :

$$l : S \rightarrow \mathbb{R}_+ \cup \{0\} \quad (6.1)$$

DEFINITION 6.2

LENGTHED SET:

a couple $(S, l) : S$ is a set and l is a length on S (6.2)

Given a set S let us define:

DEFINITION 6.3

SET OF THE PARTIAL FUNCTIONS ON S :

$$PF(S) \equiv \{\phi : S \overset{\circ}{\rightarrow} S\} \quad (6.3)$$

Given a lengthed set (S, l) let us define:

DEFINITION 6.4

DESCRIPTIVE INFORMATION ON (S, l)

W.R.T. $\phi \in PF(S)$:

$I_\phi : S \rightarrow \mathbb{R}_+ \cup \{0, \infty\}$:

$$I_\phi(y) \equiv \begin{cases} \min\{l(x) : \phi(x) = y\} & \exists x \in S : \phi(x) = y \\ +\infty & \text{otherwise.} \end{cases} \quad (6.4)$$

Given , then, a set $\mathcal{C} \subseteq PF(S)$ we can introduce on it the following partial ordering:

DEFINITION 6.5

$\phi_1 \in \mathcal{C}$ IS LESS PROLIX THAN
 $\phi_2 \in \mathcal{C}$ ($\phi_1 \leq \phi_2$) :

$$\exists c_{\phi_1, \phi_2} \in \mathbb{R}_+ : I_{\phi_1}(x) \leq I_{\phi_2}(x) + c_{\phi_1, \phi_2} \quad \forall x \in S \quad (6.5)$$

We will say, then, that:

DEFINITION 6.6

$\phi_1 \in \mathcal{C}$ AND $\phi_2 \in \mathcal{C}$ ARE EQUIVALENT
($\phi_1 \sim \phi_2$) :

$$(\phi_1 \leq \phi_2) \text{ and } (\phi_2 \leq \phi_1) \quad (6.6)$$

Let us now introduce the following basic notions:

DEFINITION 6.7

OPTIMAL DESCRIPTIVE METHOD IN \mathcal{C} :

$$\omega \in \min_{\sim}^{\mathcal{C}} \quad (6.7)$$

DEFINITION 6.8

DESCRIPTIVE INFORMATION BY \mathcal{C} IS
OBJECTIVE:

$$\exists \min_{\sim}^{\mathcal{C}} \quad (6.8)$$

Remark 6.2

PASSAGE FROM DESCRIPTIVE INFORMATION TO ALGORITHMIC INFORMATION:

Let us observe that, up to now, I have spoken about *descriptive information* and not of *algorithmic information*: in fact I have not yet introduced the more important constraint on the allowed description methods: that of being *algorithmically implementable*, or, said in a different way, to be *effectively-computable w.r.t. the informal notion of effective-computability*.

Though such a passage was proposed by A.N. Kolmogorov to bypass the problem that **descriptive information by $PF(\Sigma^*)$ was not objective** the conceptual meaning of resorting to **Computability Theory** was extraordinarily clear to the great mathematician [Shi93].

DEFINITION 6.9

C_Φ - COMPUTABLE-PARTIAL FUNCTIONS
ON S:

$$\begin{aligned} C_\Phi - PF(S) \equiv \\ \{f \in PF(S) : f \text{ is computable} \\ \text{by } \textit{classical}_\Phi \text{ computers}\} \quad (6.9) \end{aligned}$$

DEFINITION 6.10

NC_Φ - COMPUTABLE-PARTIAL FUNCTIONS
ON S:

$$\begin{aligned} NC_\Phi - PF(S) \equiv \\ \{f \in PF(S) : f \text{ is computable} \\ \text{by } \textit{nonclassical}_\Phi \text{ computers}\} \quad (6.10) \end{aligned}$$

We have now all the ingredients required to completely formalize the Uspensky's Axiomatic Procedure:

**USPENSKY'S AXIOMATIC
PROCEDURE TO INTRODUCE
PHYSICALLY-CLASSICAL AND
PHYSICALLY-NONCLASSICAL
ALGORITHMIC INFORMATION
THEORY ON A LENGTHED SET (S, l) :**

- C_Φ (NC_Φ)- ALGORITHMIC
INFORMATION THEORY ON (S, l) MAY
BE DEFINED IF AND ONLY IF
DESCRIPTIVE INFORMATION ON
 $C_\Phi - PF(S)$ ($NC_\Phi - PF(S)$) IS
OBJECTIVE

- THE C_Φ (NC_Φ)- ALGORITHMIC INFORMATION THEORY ON (S, l) IS DEFINED AS THE DESCRIPTIVE INFORMATION W.R.T. AN OPTIMAL DESCRIPTIVE METHOD IN A CERTAIN SUBSET:

$$C_\Phi - AC - AL(S) \subseteq C_\Phi - PF(S)$$

$$(NC_\Phi - AC - AL(S) \subseteq NC_\Phi - PF(S))$$

Remark 6.3

EXTENSION OF THE ABOVE CONSTRUCTION TO STRUCTURED SETS:

Eventually S might be endowed with some suppletive structure \textcircled{S} . The objects we want to describe will, then, be considered, more properly, as elements of the mathematical structure $(S, 1, \textcircled{S})$.

Our descriptive process will, then, have to take in consideration such a structure. The considered class of description-methods shall, then, consist of subsets not of $PF(S)$ but of its subset:

DEFINITION 6.11

**SET OF THE PARTIAL ISOMORPHISMS OF
 (S, \textcircled{S}) :**

$$PI(S, \textcircled{S}) \equiv \{f \in PF(S) : f \text{ is } \textcircled{S} - \text{preserving}\} \quad (6.11)$$

DEFINITION 6.12

C_Φ - COMPUTABLE-PARTIAL
ISOMORPHISMS ON (S, \otimes) :

$$\begin{aligned} C_\Phi - PI(S, \otimes) \equiv \\ \{f \in C_\Phi - PI(S) : \\ f \text{ is computable} \\ \text{by } \textit{classical}_\Phi \text{ computers}\} \quad (6.12) \end{aligned}$$

DEFINITION 6.13

NC_Φ - COMPUTABLE-PARTIAL
ISOMORPHISMS ON (S, \otimes) :

$$\begin{aligned} NC_\Phi - PI(S, \otimes) \equiv \\ \{f \in NC_\Phi - PI(S) : \\ f \text{ is computable} \\ \text{by } \textit{nonclassical}_\Phi \text{ computers}\} \quad (6.13) \end{aligned}$$

**USPENSKY'S AXIOMATIC
PROCEDURE TO INTRODUCE
PHYSICALLY-CLASSICAL AND
PHYSICALLY-NONCLASSICAL
ALGORITHMIC INFORMATION
THEORY ON A STRUCTURED LENGTHED
SET (S , 1 , \mathbb{S})**

- C_Φ (NC_Φ)- ALGORITHMIC
INFORMATION THEORY ON (S , 1 , \mathbb{S})
MAY BE DEFINED IF AND ONLY IF
DESCRIPTIVE INFORMATION ON
 $C_\Phi - PI(S, \mathbb{S})$ ($NC_\Phi - PI(S, \mathbb{S})$) IS
OBJECTIVE

- THE C_Φ (NC_Φ)- ALGORITHMIC INFORMATION THEORY ON (S , l , \mathbb{S}) IS DEFINED AS THE DESCRIPTIVE INFORMATION W.R.T. AN OPTIMAL DESCRIPTIVE METHOD IN A CERTAIN SUBSET:

$$C_\Phi - AC - AL(S, \mathbb{S}) \subseteq C_\Phi - PI(PS, \mathbb{S})$$

$$(NC_\Phi - AC - AL(S, \mathbb{S}) \subseteq NC_\Phi - PI(PS, \mathbb{S}))$$

Marian Boykan Pour-El and Jonathan Ian Richards has developed a very interesting Computability Theory on Banach Spaces [Ric89] that, under the explicit assumption of a generalization of **Church Thesis** that I will call from now on **Pour El Thesis** [PE99] characterizes mathematically:

1. a subset:

$$B_{COMP} = C_{\Phi} - B = NC_{\Phi} - B$$

of **vectors** of a **Banach space** B

2. a subset:

$$C_{\Phi} - \mathcal{L}(\mathbb{H}) = NC_{\Phi} - \mathcal{L}(\mathbb{H}) \subset \mathcal{L}(\mathbb{H})$$

of the space $\mathcal{L}(\mathbb{H})$ of the **linear operators** on a **separable Hilbert space** \mathbb{H}

that are **effectively** computable, according to the informal notion of effective computability, by any kind of physical computer (classical or nonclassical)

Given a Banach space B on the real/complex field
Pour-El and Richards introduce the following
notion:

DEFINITION 6.14

COMPUTABILITY STRUCTURE ON B :

a specification of a subset \mathcal{S} of the set B^∞ of all
the sequences in B identified as the **set of the
computable sequences on B** satisfying the
following axioms:

AXIOM 6.1

ON LINEAR FORMS:

HP:

$\{x_n\}$ and $\{y_n\}$ computable sequences in B

$\{\alpha_{n,k}\}, \{\beta_{n,k}\}$ two recursive double sequence of
real/complex numbers

d recursive function

$$s_n \equiv \sum_{k=0}^{d(n)} \alpha_{n,k} x_k + \beta_{n,k} y_k$$

TH:

$$\{s_n\} \in \mathcal{S}$$

AXIOM 6.2

ON LIMITS:

HP:

$x_{n,k}$ computable double sequence in B :

$$alg - \lim_{k \rightarrow \infty} x_{n,k} = x_n$$

TH:

$$\{x_n\} \in \mathcal{S}$$

AXIOM 6.3

ON NORMS:

HP:

$$\{x_n\} \in \mathcal{S}$$

TH:

$\{\|x_n\|\}$ is a recursive sequence of real numbers.

where:

DEFINITION 6.15

THE SEQUENCE OF RATIONAL NUMBERS $\{r_n\}$ IS COMPUTABLE:

$\exists a, b, c$ recursive functions:

$$(c_n \neq 0 \forall n) \text{ and} \quad (r_n = (-1)^{a(n)} \frac{b(n)}{c(n)}) \quad (6.14)$$

THE SEQUENCE OF RATIONAL NUMBERS $\{r_n\}$ CONVERGES ALGORITHMICALLY TO $x \in \mathbb{R}$ ($\text{alg} - \lim_{n \rightarrow \infty} r_n = x$)

$\exists f$ recursive function :

$$n \geq f(n) \Rightarrow |r_n - x| < \frac{1}{2^n} \quad (6.15)$$

DEFINITION 6.16

RECURSIVE REAL NUMBERS:

$$\mathbb{R}_{COMP} \equiv$$

$\{x \in \mathbb{R} : \exists \{r_n\} \text{ computable sequence of rationals} :$

$$\text{alg} - \lim_{n \rightarrow \infty} r_n = x\} \quad (6.16)$$

SOME PROPERTIES OF \mathbb{R}_{COMP} :

1. $(\mathbb{R}_{COMP}, +, \cdot)$ is a field

2. $\pi, e, \gamma \in \mathbb{R}_{COMP}$

3.

$$\mathbb{R}_{ALGEBRAIC} \subset \mathbb{R}_{COMP} \quad (6.17)$$

4.

$$card(\mathbb{R}_{COMP}) = \aleph_0 \quad (6.18)$$

Given a double sequence of real numbers $\{x_{n,k}\}$ and an other sequence $\{x_n\}$ of real numbers such that:

$$\lim_{k \rightarrow \infty} x_{n,k} = x_n \quad \forall n \in \mathbb{N} \quad (6.19)$$

DEFINITION 6.17

$\{x_{n,k}\}$ CONVERGES ALGORITHMICALLY TO $\{x_n\}$ ($alg - \lim_{k \rightarrow \infty} x_{n,k} = x_n$)

$\exists e : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ *recursive* :

$$(k > e(n, N) \Rightarrow |x_{n,k} - x_n| \leq \frac{1}{2^N}) \quad \forall n \in \mathbb{N}, \quad \forall N \in \mathbb{N} \quad (6.20)$$

DEFINITION 6.18

$\{x_n\}_{n \in \mathbb{N}}$ IS COMPUTABLE:

$\exists \{r_{n,k} \in \mathbb{Q}\}_{n,k \in \mathbb{N}}$ *computable* :

$$|r_{n,k} - x_n| \leq \frac{1}{2^k} \quad \forall n, k \in \mathbb{N} \quad (6.21)$$

Remark 6.4

THE COMPUTABILITY OF A SEQUENCE IS
MORE THAN THE COMPUTABILITY OF
ALL ITS ELEMENTS

given a sequence $\{x_n\}$ of real numbers, the fact that each element of the sequence is computable, and can, consequently, be effectively approximated to any desired degree of precision by a computer program P_n given in advance doesn't imply the computability of the whole sequence since there might not exist an effective way of combining the sequence of programs $\{P_n\}$ in a unique program P computing the whole sequence $\{x_n\}$.

Remark 6.4 should clarify why the definition of a computability structure on a Banach space B is made through a proper specification of the computable sequences in B and not, simply, by the specification of a proper set of the computable vectors.

The notion of a computable vector, instead, is immediately induced by the assignment on B of a computability structure \mathcal{S} .

DEFINITION 6.19

COMPUTABLE VECTORS OF B :

$$B_{COMP} \equiv \{x \in B : \{x, x, x, \dots\} \in \mathcal{S}\} \quad (6.22)$$

Remark 6.5

INTUITIVE MEANING OF THE AXIOMS

Axiom6.1, Axiom6.2 and Axiom6.3

since a Banach space is made up of:

1. a linear space V
2. a norm on V
3. the completeness-condition for such a norm

it appears natural to require analogous effective conditions for the set of computable sequences.

Remark 6.6

THE MULTIVOCITY PROBLEM FOR THE COMPUTABILITY STRUCTURE

The axioms Axiom6.1, Axiom6.2 and Axiom6.3 don't provide the axiomatic definition of a unique structure for a Banach space B since B admits, generally, more computability-structures.

This, anyway, doesn't relativize the whole approach thanks to the existence of a suppletive condition whose satisfiability results in the invoked univocity.

Given a computability structure \mathcal{S} on a Banach space B :

DEFINITION 6.20

EFFECTIVE GENERATING SET FOR B :

$$\{e_n\} \in \mathcal{S} :$$

$$\text{linear} - \text{span}(\{e_n\}) \text{ is dense in } B \quad (6.23)$$

DEFINITION 6.21

B IS EFFECTIVELY SEPARABLE:

$$\exists \{e_n\} \text{ effective generating set for } B \quad (6.24)$$

Theorem 6.1

THEOREM OF UNIVOCITY

HP:

B Banach space

\mathcal{S}_1 , \mathcal{S}_2 effectively separable computability
structures on B

$\{e_n\} \in \mathcal{S}_1 \cap \mathcal{S}_2$ effective generating set for B

TH:

$$\mathcal{S}_1 = \mathcal{S}_2$$

Remark 6.7

COMPUTABILITY STRUCTURE OF A QUANTUM SYSTEM:

Given a **quantum physical system** (\mathcal{H}, \hat{H}) the existence of an effectively measurable operator having as eigenvectors a basis $\{e_n\}$ of \mathbb{H} gives us immediately an univocal notion of computability on \mathbb{H} : that associated to the effective generating set $\{e_n\}$ (said an **effective-basis** of \mathbb{H}).

Example 6.1

SPIN $\frac{1}{2}$ SYSTEMS

Given a **quantum physical system** $(\mathcal{H} = \mathbb{C}^2, \hat{H} = f(\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z))$ since the x-component, the y-component and the z-component of the spin are observable effectively-measurable (e.g. by a Stern-Gerlach apparatus) it follows that :

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \right\}$$
$$\left\{ \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{i}{\sqrt{2}} \end{pmatrix} \right\}$$

are three **effective-bases** of \mathbb{H} .

Furthermore since also the identity operator is obviously effectively measurable it follows that $\{ \mathbb{I}, \sigma_x, \sigma_y, \sigma_z \}$ is an **effectively generating set** for the W^* -algebra $\mathcal{B}(\mathbb{H}) = M_2(\mathbb{C})$.

Given an **effectively separable Hilbert space**
 \mathbb{H}

DEFINITION 6.22

COMPUTABLE LINEAR OPERATOR ON
 \mathbb{H} ($T \in \mathcal{L}_{COMP}(\mathbb{H})$)

$T \in \mathcal{L}(\mathbb{H})$ closed, such that there exist a
 computable sequence $\{e_n\}$ in \mathbb{H} so that:

$$\{(e_n, T, e_n)\} \text{ is a computable sequence} \\
\text{of } \mathbb{H} \times \mathbb{H} \quad (6.25)$$

and:

$$\text{linear} - \text{span}\{(e_n, T, e_n)\} \text{ is dense in} \\
\text{the graph } \Gamma(T) \text{ of } T \quad (6.26)$$

Remark 6.8

INTUITIVE MEANING OF THE DEFINITION 6.22

- a **bounded operator** is computable if its action on any computable vector is effectively determinable
- an **unbounded operator** is computable if its action on any computable vector is effectively determinable and if we are able to solve effectively the **halting problem** corresponding to the belongness to its domain of definition, i.e. if we have an effective-algorithm that , given a generic computable vector x of \mathbb{H} tells us whether T halts on x ($Tx \downarrow$) or not ($Tx \uparrow$).

Remark 6.9

FACTORS AS BUILDING BLOCKS OF VON NEUMANN ALGEBRAS:

Any W^* -algebra A is a sort of direct integral of factors:

$$A = \int_{\mathcal{Z}(A)}^{\otimes} A_{\lambda} d\nu(\lambda) \quad (6.27)$$

where:

- $\mathcal{Z}(A) \equiv A \cap A'$ is the **center** of A
- the A_{λ} are all **factors**, i.e.:

$$\mathcal{Z}(A_{\lambda}) = \{\mathbb{C}\mathbb{I}\} \quad \forall \lambda \in \mathcal{Z}(A) \quad (6.28)$$

Hence the analysis of a W^* -algebra may be reduced to the analysis of its building blocks

DEFINITION 6.23

DISCRETE TYPE VON NEUMANN
ALGEBRA:

a W^* -algebra in which **factor decomposition**
eq.6.27 appear only factors of type

I_n $n \in \mathbb{N} \cup \{\infty\}$, i.e. don't appear factors of type
 II_n $n \in \{1, \infty\}$ and of type III_α $\alpha \in [0, 1]$

DEFINITION 6.24

DISCRETE TYPE NONCOMMUTATIVE
PROBABILITY SPACE:

(A, ω) noncommutative probability space with A
discrete type W^* -algebra

Remark 6.10

POUR EL THESIS TOUCHES ONLY DISCRETE TYPE NONCOMMUTATIVE PROBABILITY SPACES

Since a W^* -algebra is isomorphic to the space $\mathcal{B}(\mathbb{H})$ of the **bounded linear operators on a separable Hilbert space** \mathbb{H} if and only if it is of **discrete type** [Ben93] it follows that Pour El Thesis implies the following relations:

$$\begin{aligned} C_{\Phi} - AUT(A) &= NC_{\Phi} - AUT(A) \\ &= AUT(A) \cap \mathcal{L}_{COMP}(A) \end{aligned} \tag{6.29}$$

$$\begin{aligned} C_{\Phi} - DYN[(A, \omega)] &= NC_{\Phi} - DYN[(A, \omega)] \\ &= DYN[(A, \omega)] \cap \mathcal{L}_{COMP}(A) \end{aligned} \tag{6.30}$$

if and only if (A, ω) is a noncommutative probability space of discrete type

7 Looking for Martin-Löf physically-quantum randomness: an issue of Algorithmic Free Probability Theory

Given the unbiased noncommutative probability space $(L^\infty(\Sigma_{NC}^\infty), \tau_{unbiased})$ of the sequences on the one qubit noncommutative alphabet Σ_{NC} :

DEFINITION 7.1

UNARY PREDICATES ON $L^\infty(\Sigma_{NC}^\infty)$:

$$\begin{aligned} \mathcal{P}(L^\infty(\Sigma_{NC}^\infty)) &\equiv \\ &\{p_{\bar{x}} : \text{predicate about} \\ &\bar{x} \in L^\infty(\Sigma_{NC}^\infty)\} \quad (7.1) \end{aligned}$$

DEFINITION 7.2

Q_Φ - ALGORITHMICALLY TYPICAL
PROPERTIES OF $L^\infty(\Sigma_{NC}^\infty)$:

$$Q_\Phi - \mathcal{P}(L^\infty(\Sigma_{NC}^\infty))_{ALG-TYPICAL} \equiv$$

$$\{ p_{\bar{x}} \in \mathcal{P}(L^\infty(\Sigma_{NC}^\infty)) :$$

$$\{ \bar{x} \in L^\infty(\Sigma_{NC}^\infty) : p_{\bar{x}} \text{ doesn't hold } \}$$

$$\text{is a } Q_\Phi\text{-algorithmically null set} \} \quad (7.2)$$

where Q_Φ - **ALGORITHMICALLY** refers to
computability by *physical computers*
obeying *Nonrelativistic or Partial*
Relativistic Quantum Mechanics

DEFINITION 7.3

RANDOM SEQUENCES OF QUBITS :

$$Q_{\Phi} - RANDOM(L^{\infty}(\Sigma_{NC}^{\infty})) \equiv$$

$$L^{\infty}(\Sigma_{NC}^{\infty}) - \{A \subset L^{\infty}(\Sigma_{NC}^{\infty})$$

$$Q_{\Phi}\text{- algorithmically null } \} \quad (7.3)$$

Remark 7.1

WHAT LACKS TO COMPLETE DEFINITION 7.3

Clearly the definition 7.3 is uncomplete until one gives the definition of Q_Φ - algorithmically null subsets of $L^\infty(\Sigma_{NC}^\infty)$.

INGREDIENTS USEFUL TO IDENTIFY THE
 CORRECT NOTION OF
 Q_Φ -ALGORITHMICALLY NULL SUBSETS OF
 $L^\infty(\Sigma_{NC}^\infty)$:

1. the Pour - El Richards Theory
2. the constraint 3.2
3. the link exististing between **algorithmic
 comprimibility** and **probabilistic
 trasmission comprimibility** of a sequence
 of qubits

Remark 7.2

WHAT POUR EL - RICHARDS THEORY CAN TELL ON THE COMPUTABILITY THEORY OF THE SEQUENCES ON THE ONE QUBIT NONCOMMUTATIVE ALPHABET:

Since $(L^\infty(\Sigma_{NC}^\infty), \tau_{unbiased})$ is not of discrete type Pour El Thesis can't be advocated to identify $\mathcal{L}(L^\infty(\Sigma_{NC}^\infty))_{COMP}$ and thus to construct Algorithmic Information Theory on the sequences over Σ_{NC} .

Anyway since an infinite chain of spin $\frac{1}{2}$ at infinite temperature is a **quantum physical system** described exactly by the unbiased noncommutative probability space

$(L^\infty(\Sigma_{NC}^\infty), \tau_{unbiased})$ of the sequences on the one qubit noncommutative alphabet Σ_{NC} it follows, looking at the example6.1, that

$\otimes_{n \in \mathbb{N}} \{ \mathbb{I}, \sigma_x, \sigma_y, \sigma_z \}$ is an **effectively generating set** of $L^\infty(\Sigma_{NC}^\infty)$ and thus, for the theorem6.1, individuates on it a **computability structure**

Remark 7.3

NOT TRIVIALITY OF TRANSLATING CONSTRAINT3.2 IN TERMS OF TYPICAL PROPERTIES

In the commutative case we saw that the constraint3.1 could simply be translated in terms of typical properties as the constraint4.1.

If the definition2.8 involved **free product**[Pet00] instead of **tensor products** of W^* -algebras the same would happen also for the constraint3.2, i.e. such a constraint could be simply stated as:

CONSTRAINT 7.1

ERRONEOUS WAY OF LOOKING FOR THE
DEFINITION OF $RANDOM(\Sigma_{NC}^\infty)$:

the unary predicate

$p_{\bar{x}} \equiv \langle\langle \bar{x} \in RANDOM(\Sigma_{NC}^\infty) \rangle\rangle$ is a
 Q_Φ -typical property of Σ_{NC}^∞ , i.e.

$p_{\bar{x}} \in Q_\Phi - \mathcal{P}(\Sigma_{NC}^\infty)_{TYPICAL}$

Called $c_n \in \Sigma$ the random variable on the **unbiased probability space on the one cbit alphabet** $(\Sigma, C_{\frac{1}{2}, \frac{1}{2}})$ corresponding to the result of the toss of a **classical coin** made at time $n \in \mathbb{N}$:

DEFINITION 7.4

**NORMALIZED INDEPENDENT-LETTERS
CLASSICAL INFORMATION SOURCE:**

the $\{c_n\}$, supposed to be an **independent sequence** on $(\Sigma, C_{\frac{1}{2}, \frac{1}{2}})$ so that:

$$\begin{aligned} E(c_n) &= 0 \quad \forall n \in \mathbb{N} \\ E(c_n^2) &= 1 \quad \forall n \in \mathbb{N} \end{aligned} \tag{7.4}$$

An immediate argument of **Commutative Large Deviation Theory** leads to **Shannon's Noiseless - Memoryless Coding Theorem** [Khi57], [Bil65], [Tho91], [Kak99] implying that the **probabilistic transmission-comprimibility** for such a classical information source is:

$$S_{Shannon}(C_{\frac{1}{2}, \frac{1}{2}}) = 1 \frac{cbit}{letter} \quad (7.5)$$

Called $c_n \in M_2(\mathbb{C})$ the noncommutative random variable on the **unbiased noncommutative probability space on the one qubit alphabet** $(M_2(\mathbb{C}), \tau_2)$ corresponding to the result of the toss of a **quantum coin** made at time $n \in \mathbb{N}$:

DEFINITION 7.5

**NORMALIZED INDEPENDENT-LETTERS
QUANTUM INFORMATION SOURCE:**

the $\{c_n\}$, supposed to be an **independent sequence** on $(M_2(\mathbb{C}), \tau_2)$ so that:

$$\begin{aligned}\tau_2(c_n) &= 0 \quad \forall n \in \mathbb{N} \\ \tau_2(c_n^2) &= 1 \quad \forall n \in \mathbb{N}\end{aligned}\tag{7.6}$$

DEFINITION 7.6

NORMALIZED FREE-LETTERS QUANTUM
INFORMATION SOURCE:

the $\{c_n\}$, supposed to be a **free sequence** on
 $(M_2(\mathbb{C}), \tau_2)$ so that:

$$\begin{aligned}\tau_2(c_n) &= 0 \quad \forall n \in \mathbb{N} \\ \tau_2(c_n^2) &= 1 \quad \forall n \in \mathbb{N}\end{aligned}\tag{7.7}$$

Remark 7.4

NOISELESS CODING THEOREM REGARDS THE INDEPENDENT-LETTERS QUANTUM INFORMATION SOURCES AND NOT THE FREE-LETTERS QUANTUM INFORMATION SOURCES

The **Noncommutative Large Deviation Theory's** argument [Pet93], [Pet00] leading to **Schumacher's Noiseless-Memoryless Quantum Coding Theorem** [Joz97], [Sch98], [Pre98], [Win99], [Pet99] implies that the **probabilistic transmission-comprimibility** of the **normalized independent letters quantum information source** is:

$$S_{Von\ Neumann}(\tau_2) = 1 \frac{qubit}{letter} \quad (7.8)$$

*But Schumacher's Theorem can't, obviously, be applied to the **free-letters-quantum information source** whose relevant large deviation theoretical entropy-functional is Voiculescu's **free entropy** [Pet00]*

Remark 7.5

COMMUTATIVE VERSUS NONCOMMUTATIVE LARGE DEVIATIONS FROM THE CENTRAL LIMITS

The conceptual meaning of the Noiseless Coding Theorem for any (classical or quantum) information source IS is:

- the exponential decay of probability of large deviations from the **IS - central limit measure** $P_{central}$ is governed by some **large deviation theoretical entropy-functional** $S_{IS}[P]$

- the consequential possibility of not-codifying the S_{IS} - not typical messages during the trasmission of information with asymptotically null misunderstanding-error
- the resulting $S_{IS}[P_{IS}]$ **probabilistic trasmission comprimibility** for IS

So it is important, first of all, to compare the Central Limit Theorems of Commutative and Noncommutative Probability Theory

Theorem 7.1

CENTRAL LIMIT FOR THE NORMALIZED
LETTERS-INDEPENDENT CLASSICAL
INFORMATION SOURCE

HP:

$\{c_n\}$ letters-independent classical information
source

$$m_n \equiv \frac{1}{\sqrt{n}} \sum_{k=1}^n c_k$$

$$\sup_n |E(c_n^k)| < +\infty \quad \forall k \in \mathbb{N}$$

TH:

$meas - \lim_{n \rightarrow \infty} m_n =$ **standard gaussian
measure**

Theorem 7.2

CENTRAL LIMIT FOR THE NORMALIZED LETTERS-FREE QUANTUM INFORMATION SOURCE

HP:

$\{c_n\}$ letters-free quantum information source

$$m_n \equiv \frac{1}{\sqrt{n}} \sum_{k=1}^n c_k$$

$$\sup_n |\tau_2(c_n^k)| < +\infty \quad \forall k \in \mathbb{N}$$

TH:

$$\text{meas} - \lim_{n \rightarrow \infty} m_n = \text{standard semicircle measure}$$

with:

DEFINITION 7.7

GAUSSIAN MEASURE OF MEAN m AND
VARIANCE σ^2 :

the probability measure on $(\mathbb{R}, \mathcal{F}_{Borel})$ with
density:

$$g(m, \sigma; x) \equiv \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-m)^2}{2\sigma^2}} \quad (7.9)$$

DEFINITION 7.8

STANDARD GAUSSIAN MEASURE:

the probability measure on $(\mathbb{R}, \mathcal{F}_{Borel})$ with
density $g(0, 1; x)$

DEFINITION 7.9

SEMICIRCLE MEASURE OF MEAN m AND
VARIANCE $\frac{r^2}{4}$:

the probability measure on $(\mathbb{R}, \mathcal{F}_{Borel})$ with
density:

$$sc(m, r; x) \equiv$$

$$\begin{cases} \frac{2}{\pi r^2} \sqrt{r^2 - (x - m)^2} & \text{if } m - r \leq x \leq m + r, \\ 0 & \text{otherwise.} \end{cases} \quad (7.10)$$

DEFINITION 7.10

STANDARD SEMICIRCLE MEASURE:

the probability measure on $(\mathbb{R}, \mathcal{F}_{Borel})$ with
density $sc(0, 2; x)$

MOMENTS OF THE STANDARD GAUSSIAN MEASURE :

$$M_n [g(0, 1; x)] \equiv \int_{-\infty}^{+\infty} dx x^n g(0, 1; x) = \begin{cases} (2k - 1) !! & \text{if } n = 2k, k \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases} \quad (7.11)$$

MOMENTS OF THE STANDARD SEMICIRCLE MEASURE :

$$M_n [sc(0, 2; x)] \equiv \int_{-\infty}^{+\infty} dx x^n sc(0, 2; x) = \begin{cases} \frac{1}{k+1} \binom{2k}{k} & \text{if } n = 2k, k \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases} \quad (7.12)$$

Remark 7.6

PROBABILISTIC ORIGIN OF WIGNER'S THEOREM ON RANDOM MATRICES:

Random matrices belonging to the Gaussian Unitary Ensemble are asymptotically-free random variables and consequently satisfy the Free Central Limit Theorem resulting in Wigner's Theorem [Pet00],[Meh91]

Given a classical probability space (Ω, P) :

DEFINITION 7.11

NONCOMMUTATIVE PROBABILITY SPACE
OF $n \times n$ RANDOM MATRICES W.R.T.
 (Ω, P) :

RANDOM-MATRICES $[n, (\Omega, P)] \equiv (A, \tau)$
with:

$A \equiv \{X \text{ } n \times n \text{ matrix} :$

$$X_{ij} \in L^\infty(\Omega, P)$$

$$i, j = 1, \dots, n\} \quad (7.13)$$

τ tracial state on A :

$$\tau(X) \equiv \frac{1}{n} \sum_{i=1}^n E(X_{ii}) \quad (7.14)$$

Given

$X \in RANDOM - MATRICES[n, (\Omega, P)]:$

DEFINITION 7.12

EMPIRICAL EIGENVALUE DISTRIBUTION
OF X :

$$\mu_{emp}(X) \equiv \frac{1}{n} \sum_{i=1}^n \delta(\lambda_i(X)) \quad (7.15)$$

DEFINITION 7.13

MEAN EIGENVALUE DISTRIBUTION OF X :

$$\mu_{mean}(X) \equiv E(\mu_{emp}(X)) \quad (7.16)$$

where $\lambda_1(X), \dots, \lambda_n(X)$ are the (random)
eigenvalues of X

DEFINITION 7.14

n - DIMENSIONAL GAUSSIAN UNITARY
ENSEMBLE :

$GUE_n \equiv$

RANDOM – MATRICES $[n, (\Omega, P)]$ where
 (Ω, P) is so that given $H \in GUE_n$:

- $H^\dagger = H$ with probability one
- $\{ \Re(H_{ij}) : i, j = 1, \dots, n \} \cup \{ \Im(H_{ij}) : i, j = 1, \dots, n \}$ is a family of independent Gaussian random variables
-

$$E(H_{ij}) = 0 \quad 1 \leq i \leq j \leq n \quad (7.17)$$

$$E(H_{ij}^2) = \frac{1}{n} \quad 1 \leq i \leq j \leq n \quad (7.18)$$

$$E(\Re(H_{ij}^2)) = E(\Im(H_{ij}^2)) = \frac{1}{2n} \quad 1 \leq i \leq j \leq n \quad (7.19)$$

References

- [Aul00] G. Auletta. *Foundations and Interpretation of Quantum Mechanics*. World Scientific, 2000.
- [Bel93] J.S. Bell. *Speakable and unspeakable in quantum mechanics*. Cambridge University Press, Cambridge, 1993.
- [Ben93] F. Benatti. *Deterministic Chaos in Infinite Quantum Systems*. Springer Verlag, Berlin, 1993.
- [Bil65] P. Billingsley. *Ergodic Theory and Information*. John Wiley and Sons Inc., 1965.
- [Cal94] C. Calude. *Information and Randomness*. Springer Verlag, Berlin, 1994.
- [Cha69a] G.J. Chaitin. On the length of programs for computing finite binary

sequences. *J. Assoc. Comput. Mach.*, 13:547–569, 1969.

[Cha69b] G.J. Chaitin. On the length of programs for computing finite binary sequences: statistical considerations. *J. Assoc. Comput. Mach.*, 16:145–159, 1969.

[Cha87] G.J. Chaitin. *Algorithmic Information Theory*. Cambridge University Press, Cambridge, 1987.

[Chu40] A. Church. On the concept of a random sequence. *J. Assoc. Comput. Mach.*, (16):145–159, 1940.

[Cle98] C.P. Williams S.H. Clearwater. *Explorations in Quantum Computing*. Springer-Verlag, New York, 1998.

[Deu85] D. Deutsch. Quantum theory, the Church-Turing principle and the

universal quantum computer. *Proc. R. Soc. Lond. A*, 400:97–117, 1985.

- [Fey82] R. Feynman. Simulating physics with computers. *Int. Jour. Theor. Physics*, 21:467–488, 82.
- [Hil93] D. Bohm B.J. Hiley. *The Undivided Universe*. Routledge, London, 1993.
- [Hol99] A.S. Holevo. Lectures on Statistical Structure of Quantum Theory.
available at the web-link
http://134.169.50.206/skripte_.html,
March 1999.
- [Joz97] R. Jozsa. Information theoretic interpretation of Von Neumann entropy. In O. Hirota A.S. Holevo C.M. Caves, editor, *Quantum Communication, Computing and Measurement*. Plenum Press, New York, 1997.

- [Joz98] R. Jozsa. Entanglement and quantum computation. In K.P. Tod S.A. Huggett, L.J. Mason, editor, *The Geometric Universe: Science, Geometry and the work of Roger Penrose*. Oxford University Press, Oxford, 1998.
- [Kak99] Y. Kakiyama. *Abstract Methods in Information Theory*. World Scientific, Singapore, 1999.
- [Khi57] A.I. Khinchin. *Mathematical Foundations of Information Theory*. Dover Publications Inc., New York, 1957.
- [Lon92] L. Longpré. Resources bounded Kolmogorov complexity and statistical tests. In O. Watanabe, editor, *Kolmogorov Complexity and Computational Complexity*, pages 66–84. Springer-Verlag, Berlin, 1992.

- [Man] Yu.I. Manin. Classical computing, quantum computing and Shor's factoring algorithm.
quant-ph/9903008. talk given at the Bourbaki Seminar , 12-13 June 1999 at the Institute Henri Poincaré, Paris.
- [Meh91] M.L. Mehta. *Random Matrices*. Academic Press, London, 1991.
- [Mey95] P.A. Meyer. *Quantum Probability for Probabilists*, volume 1538 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1995.
- [Mis81] R. Von Mises. *Probability, Statistics and Truth*. Dover Publications Inc., New York, 1981.
- [ML66a] P. Martin-Lof. The definition of random sequences. *Inform. Contr.*, 9:602–619, 1966.

- [ML66b] P. Martin-Lof. On the concept of a random sequence. *Theory Probability Appl.*, 11:177–179, 1966.
- [Odi89] P. Odifreddi. *Classical Recursion Theory: vol. 1*. Elsevier Science, Amsterdam, 1989.
- [Odi96] P. Odifreddi. Kreisel’s Church. In P. Odifreddi, editor, *Kreiseliana*, pages 389–415. A.K. Peters Ltd., Wellesley MA, 1996.
- [Odi99] P. Odifreddi. *Classical Recursion Theory: vol. 2*. Elsevier Science, Amsterdam, 1999.
- [Ohy97] R.S. Ingarden A. Kossakowski M. Ohya. *Information Dynamics and Open Systems*. Kluwer Academic Publishers, Dordrecht, 1997.

- [Opr94] I. Cuculescu A.G. Oprea.
Noncommutative Probability. Kluwer
Academic Publisher, Dordrecht, 1994.
- [Par92] K.R. Parthasarathy. *An Introduction to
Quantum Stochastic Calculus*.
Birkhauser, Basel, 1992.
- [PE99] M.B. Pour-El. The structure of
computability in analysis and physical
theory: an extension of Church's thesis.
In E.R. Griffor, editor, *Handbook of
Computability Theory*, pages 449–472.
Elsevier Science B.V., 1999.
- [Pen89] R. Penrose. *The Emperor's New Mind*.
Oxford University Press, Oxford, 1989.
- [Pen96] R. Penrose. *Shadows of the mind*.
Oxford University Press, Oxford, 1996.
- [Per95] A. Peres. *Quantum Theory: Concepts
and Methods*. Kluwer Academic
Publishers, 1995.

- [Pet93] M. Ohya D. Petz. *Quantum Entropy and Its Use*. Springer-Verlag, Berlin, 1993.
- [Pet99] D. Petz M. Mosonyi. Stationary quantum source coding. *quant-ph/9912103*, 1999.
- [Pet00] F. Hiai D. Petz. *The Semicircle Law, Free Random Variables and Entropy*. American Mathematical Society, 2000.
- [Pre98] J. Preskill. Quantum information and computation. available at the web-link: <http://www.theory.caltech.edu/~preskill/ph229>, september 1998.
- [Ric89] M.B. Pour-El J.I. Richards. *Computability in Analysis and Physics*. Springer-Verlag, Berlin, 1989.
- [Sch98] B. Schumacher. Quantum information theory. available at the web-link:

<http://topaz.kenyon.edu/people/schumacb/>, May-June 1998.

- [Shi93] A.N. Shirayayev. *Selected Works of A.N. Kolmogorov - Volume3: Information Theory and the Theory of Algorithms*. Kluwer Academic Publishers, Dordrecht, 1993.
- [Sma92] S. Smale. Theory of computation. In C. Casacuberta M. Castellet, editor, *Mathematical Research Today and Tomorrow. Viewpoints of Seven Fields Medalists*, pages 59–69. Springer-Verlag, Berlin, 1992.
- [Sol77] R.M. Solovay. On random r.e. sets. In A.I. Arruda et al., editor, *Non-Classical Logic, Model Theory and Computability*, pages 283–307. North-Holland, 1977.

- [S.S98] L.Blum F.Cucker M.Shub S.Smale.
Complexity and real computation.
Springer-Verlag, New York, 1998.
- [Sun87] V.S. Sunder. *An Invitation to von Neumann Algebras.* Springer-Verlag, New York, 1987.
- [Svo96] K. Svozil. Quantum algorithmic information theory. *Journal of Universal Computer Science*, 2:311–346, 1996.
- [Svo98] K. Svozil. *Quantum Logic.* Springer-Verlag, Singapore, 1998.
- [Tho91] T.M. Cover J.A. Thomas. *Elements of Information Theory.* John Wiley and sons, 1991.
- [Usp92] V.A. Uspensky. Complexity and entropy: An introduction to the theory of Kolmogorov complexity. In O. Watanabe, editor, *Kolmogorov*

Complexity and Computational Complexity, pages 85–102.
Springer-Verlag, 1992.

- [Vaz97] E. Bernstein U. Vazirani. Quantum complexity theory. *SIAM Journal of Computing*, 26(5):1411–1473, 1997.
- [vDSL00] A. Berthiaume W. van Dam
S. Laplante. Quantum Kolmogorov complexity. *quant-ph/0005018*, May 2000.
- [Vit97] M. Li P. Vitanyi. *An Introduction to Kolmogorov Complexity and Its Applications*. Springer Verlag, New York, 1997.
- [Vit99] P. Vitanyi. Two approaches to the quantitative definition of information in an individual pure quantum state. *quant-ph/9907035*, July 1999.

- [Win99] A. Winter. Coding theorems of quantum information theory. *quant-ph/9907077*, April 1999.
- [Zur83] J.A. Wheeler W.H. Zurek. *Quantum Theory and Measurement*. Princeton University Press, Princeton, 1983.